IN THE CLAIMS:

1. (currently amended) A method, ~~for providing an application for installation and execution on a terminal device, the terminal device being arranged with a secure environment to which access is strictly controlled by a terminal device processor, the method~~ comprising:

~~securely providing the terminal device with an encrypted application from a server device via a secure channel for said installation and execution on said device;~~

receiving, ~~at said~~in a secure environment in a terminal, via a secure channel, from a server ~~device~~outside said terminal, a first key for decrypting ~~said~~an encrypted application;

decrypting, in the secure environment, said encrypted application by means of said first key;

re-encrypting, in said secure environment, the application by means of a second key; and

storing, outside said secure environment, the re-encrypted application.

2. (currently amended) A method, ~~for providing an application for installation and execution on a terminal device, the terminal device being arranged with a secure environment to which access is strictly controlled by a terminal device processor, the method~~ comprising:

~~providing the device with~~receiving an encrypted application in a terminal;

receiving, ~~at said~~in a secure environment in said terminal, via a secure channel, from a server ~~device~~outside said terminal, a first key for decrypting said encrypted application;

encrypting, in said secure environment, said first key by means of a second key; and

storing, outside said secure environment, the encrypted first key.

3. (previously presented) The method according to claim 1, the method comprising:

encrypting, in said secure environment, said first key by means of the second key; and

storing, outside said secure environment, the encrypted first key.

4. (previously presented) The method according to claim 1, wherein said second key is symmetric and can be derived from the application.

5. (previously presented) The method according to claim 4, wherein said second key is comprised in the application itself.

6. (previously presented) The method according to claim 4, wherein said second key is generated in the secure environment using an application seed.

7. (original) The method according to claim 1, wherein multiple keys can be transferred successively on the secure channel into the secure environment, each key being used to decrypt a corresponding encrypted application in the secure environment.

8. (currently amended) Apparatus, ~~system arranged to provide an application for installation and execution on a device, the device being arranged with a secure environment to which access is controlled by a device processor, the system~~ comprising:

~~a server for securely providing the device with an encrypted application via a secure channel for said installation and execution on said terminal device;~~

an application including an installation part for receiving, ~~at said~~in a secure environment of a terminal, via ~~said~~a secure channel, from ~~said~~a server ~~device~~outside said terminal, a first key for decrypting ~~said~~an encrypted application;

a processor for decrypting, in the secure environment, said encrypted application by means of said first key;

said processor for re-encrypting, in said secure environment, the application based on a second key; and

a memory for storing, outside said secure environment, the re-encrypted application.

9. (currently amended) Apparatus, ~~system arranged to provide an application for installation and execution on a terminal device, the terminal device being arranged with a secure environment to which access is controlled by a terminal device processor, the system~~ comprising:

~~a server for providing the device with an encrypted application via a secure channel for said installation and execution on said terminal device;~~

an application including an installation part ~~of an application~~ for receiving, ~~at said~~in a secure environment of a terminal, via ~~said~~a secure channel, from ~~said~~a server ~~device~~outside said terminal, a first key for decrypting ~~said~~an encrypted application;

a processor for encrypting, in said secure environment, said first key by means of a second key; and

said processor for storing in a memory of said terminal ~~device~~, outside said secure environment, the encrypted first key.

10. (currently amended) The apparatus ~~system~~ according to claim 8, wherein said processor is:

for encrypting, in said secure environment, said first key by means of the second key; and

for storing, outside said secure environment, the encrypted first key.

11. (currently amended) The apparatus ~~system~~ according to claim 8, wherein said second key is symmetric and can be derived from the application.

12. (currently amended) The apparatus ~~system~~ according to claim 11, wherein said second key is comprised in the application itself.

13. (currently amended) The apparatus ~~system~~ according to claim 11, wherein said

second key is generated in the secure environment using an application seed.

14. (currently amended) The apparatus ~~system~~ according to claim 8, wherein the apparatus ~~system~~ is arranged such that multiple keys can be transferred successively on the secure channel into the secure environment, each key being used to decrypt a corresponding encrypted application in the secure environment.

15. (previously presented) The method of claim 2, wherein said second key is symmetric and can be derived from the application.

16. (previously presented) The method of claim 15, wherein said second key is comprised in the application itself.

17. (previously presented) The method of claim 15, wherein said second key is generated in the secure environment using an application seed.

18. (Original) The method of claim 2, wherein multiple keys can be transferred successively on the secure channel into the secure environment, each key being used to decrypt a corresponding encrypted application in the secure environment.

19. (previously presented) The method of claim 9, wherein said second key is symmetric and can be derived from the application.

20. (previously presented) The method of claim 19, wherein said second key is comprised in the application itself.

21. (currently amended) The method of claim 9, wherein the ~~system~~apparatus is arranged such that multiple keys can be transferred successively on the secure channel into the secure environment, each key being used to decrypt a corresponding encrypted application in the secure environment.

22. (currently amended) A terminal device comprising:

an installation part of an application ~~secure channel~~, responsive to ~~an encrypted~~a first key ~~downloaded~~provided over a secure channel from a server external to said terminal device for providing said ~~encrypted~~ first key ~~over said secure channel~~; and

a secure environment, responsive to said ~~encrypted~~ first key ~~received over said secure channel~~from said installation part of said application ~~within said terminal device~~ for decrypting ~~said encrypted first key for decrypting a protected application part of~~ an encrypted application in said terminal device using said first key received over said secure channel from said server external to said terminal device.

23. (previously presented) The terminal device of claim ~~21~~22, wherein said first key is encrypted by said server using a ~~private~~second key belonging to said terminal device for providing said first key from said server to said terminal device.

24. (previously presented) An integrated circuit for installation in a terminal comprising a signal processor and a secure environment, said secure environment responsive to ~~an encrypted~~ a first key from a server outside said terminal received over a secure channel for decrypting ~~said first key~~an encrypted application within said secure environment ~~for decrypting an application~~, for executing said decrypted application within said secure environment and for ~~re-encrypting~~ encrypting said first key with a second key belonging to said terminal device for storage ~~on said terminal device~~ outside said secure environment so that said first key can be used again within said secure environment without need for receipt again of said first key from said server.